"GENERATION OF CRYPTOGRAPHICALLY STRONG RANDOM NUMBERS USING MISRS"
Inventor - Richard M. Butler
Docket No. - 10991268-3

1/4
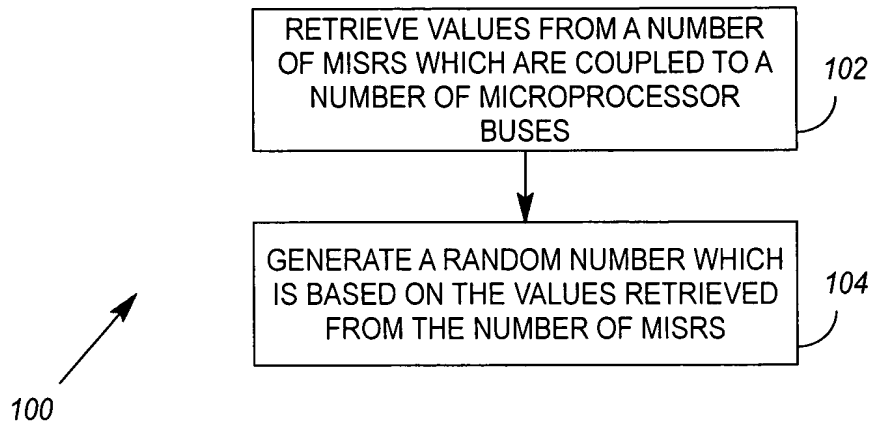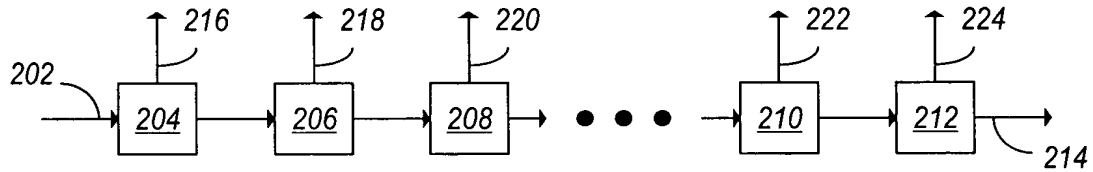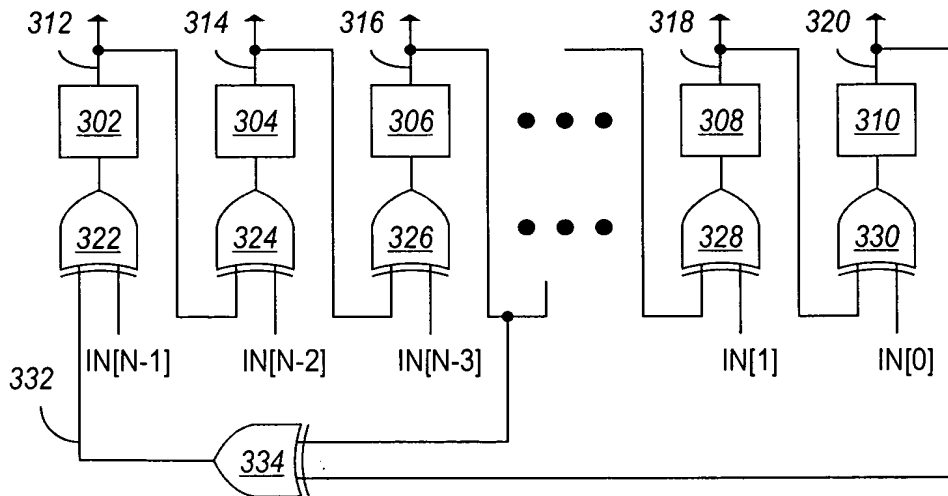
RETRIEVE VALUES FROM A NUMBER OF MISRS WHICH ARE COUPLED TO A NUMBER OF MICROPROCESSOR BUSES — 102

GENERATE A RANDOM NUMBER WHICH IS BASED ON THE VALUES RETRIEVED FROM THE NUMBER OF MISRS — 104

100

FIG. 1

216 218 220 222 224

202

204 206 208 • • • • 210 212

214

200

Prior Art

FIG. 2

312 314 316 318 320

302 304 306 • • • 308 310

322 324 326 • • • 328 330

IN[N-1] IN[N-2] IN[N-3] IN[1] IN[0]

332

334

Prior Art

FIG. 3

300

"GENERATION OF CRYPTOGRAPHICALLY STRONG RANDOM NUMBERS USING MISRS"
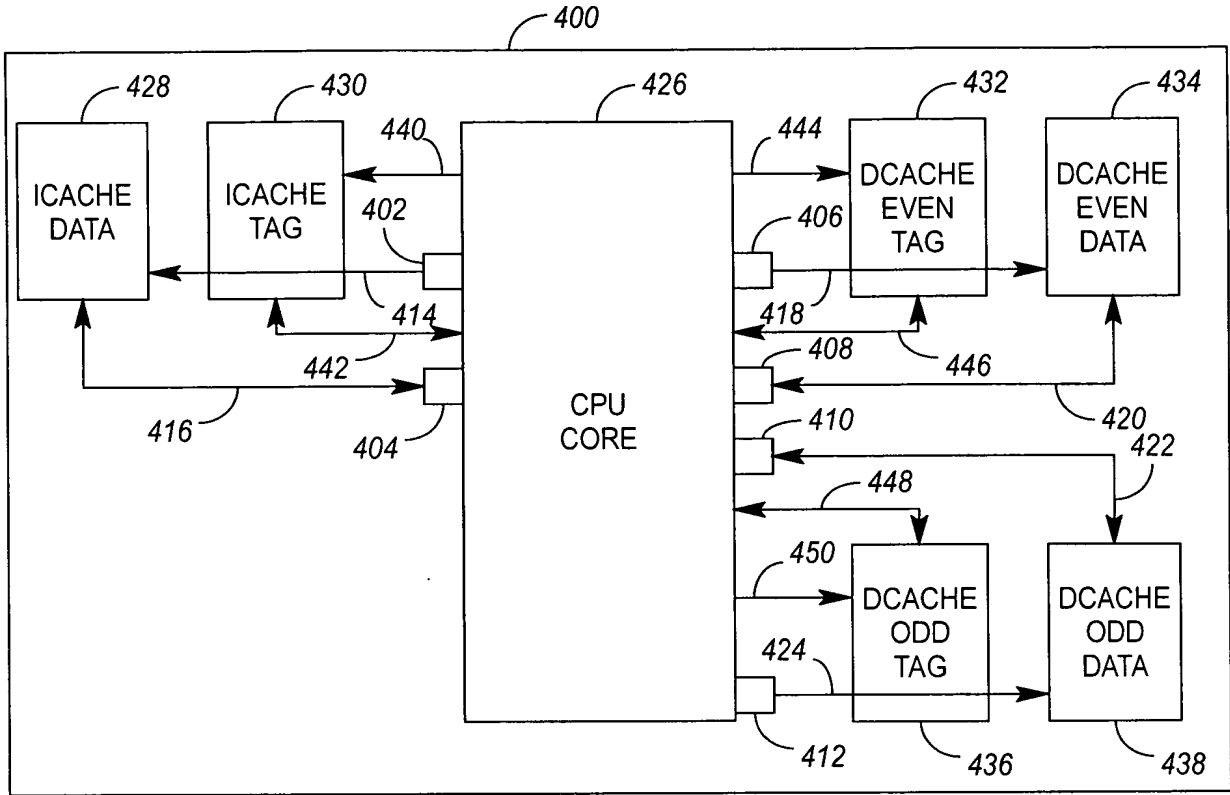Inventor - Richard M. Butler
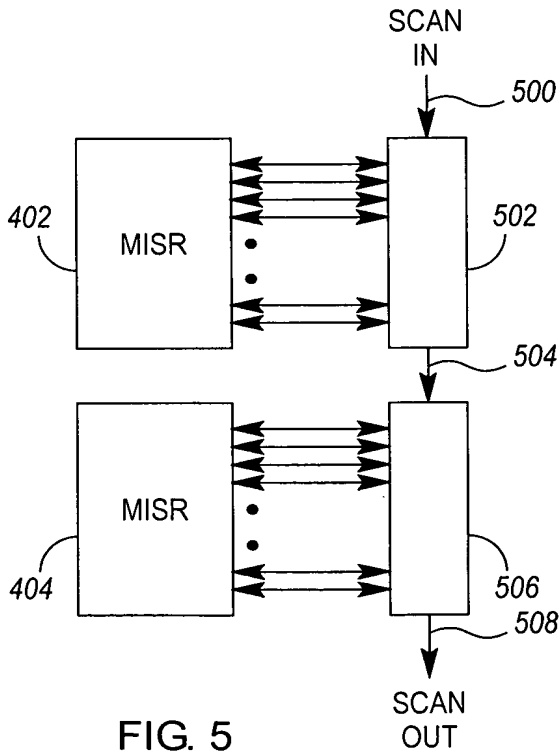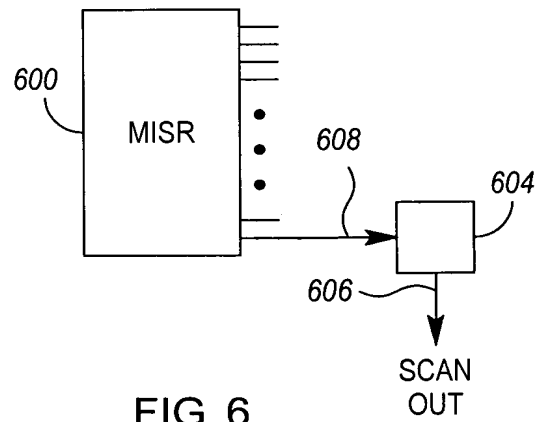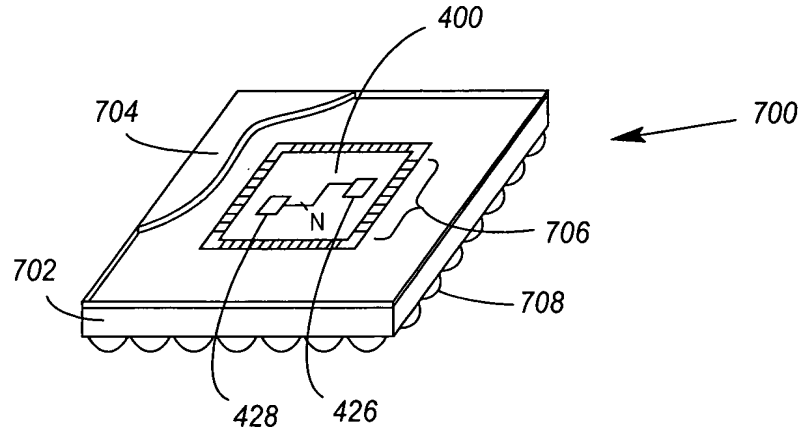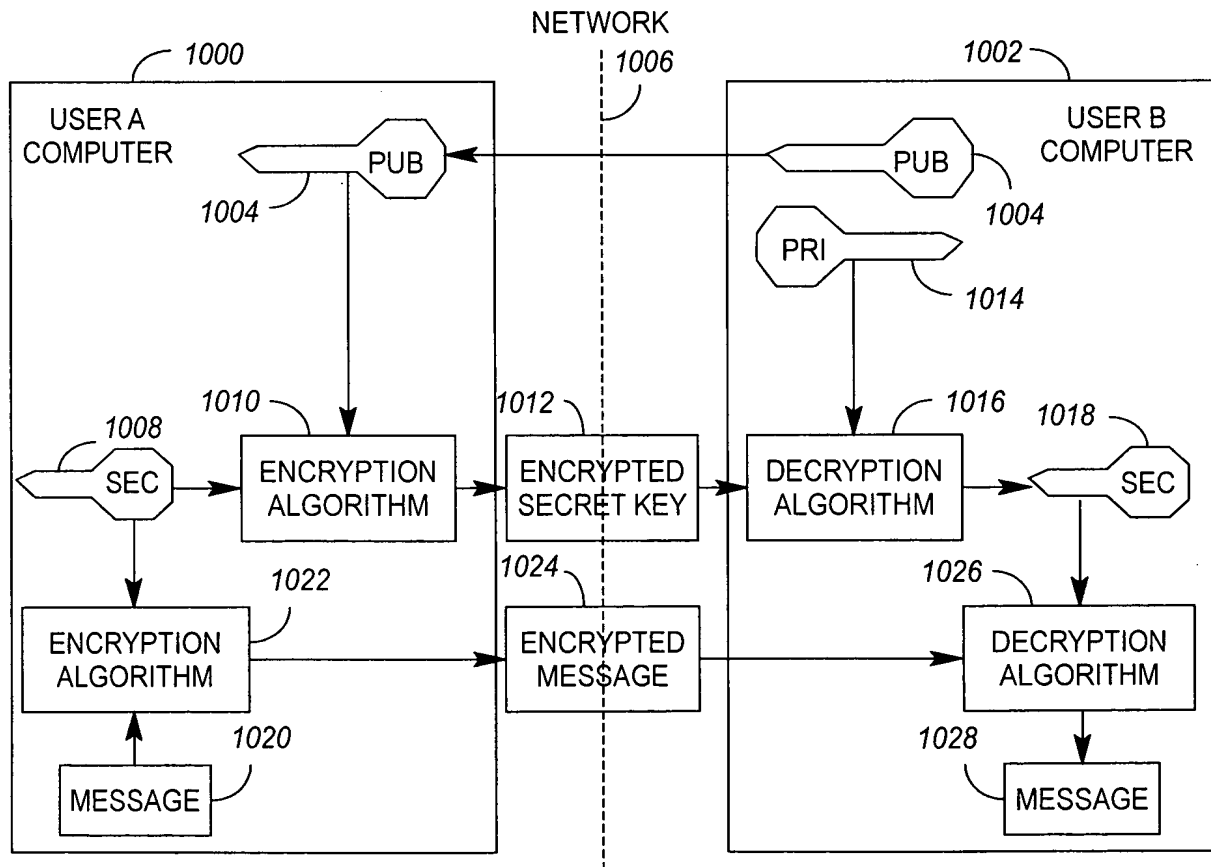Docket No. - 10991268-3

2/4

FIG. 4

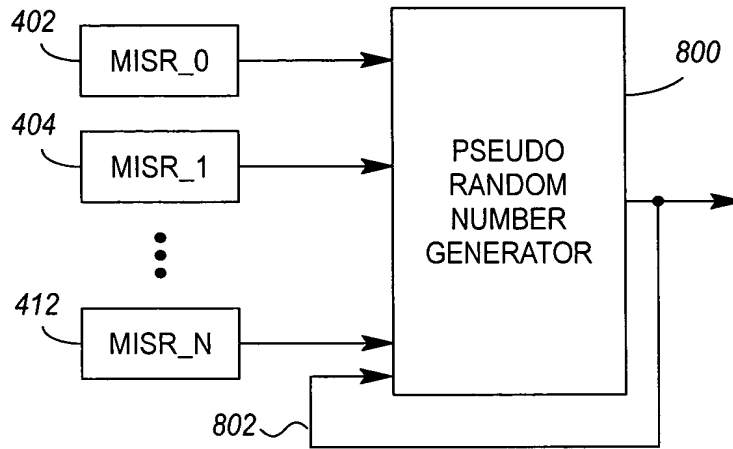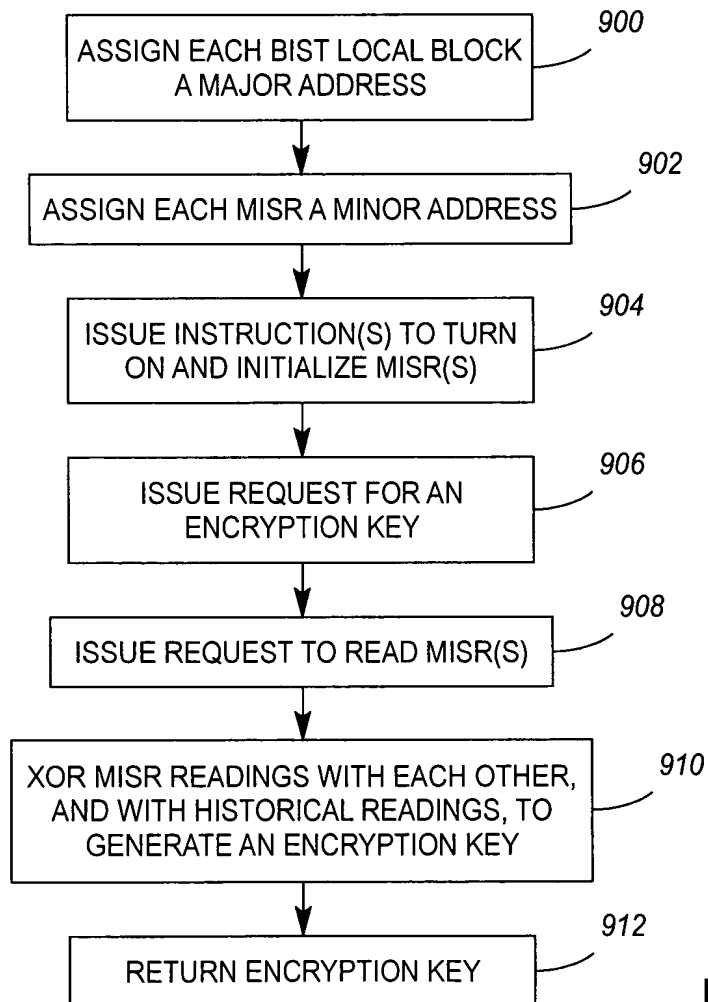

FIG. 5

FIG. 6

3/4

FIG. 7

FIG. 10

402 — MISR_0

404 — MISR_1

412 — MISR_N

800

PSEUDO RANDOM NUMBER GENERATOR

802

FIG. 8

900 — ASSIGN EACH BIST LOCAL BLOCK A MAJOR ADDRESS

902 — ASSIGN EACH MISR A MINOR ADDRESS

904 — ISSUE INSTRUCTION(S) TO TURN ON AND INITIALIZE MISR(S)

906 — ISSUE REQUEST FOR AN ENCRYPTION KEY

908 — ISSUE REQUEST TO READ MISR(S)

910 — XOR MISR READINGS WITH EACH OTHER, AND WITH HISTORICAL READINGS, TO GENERATE AN ENCRYPTION KEY

912 — RETURN ENCRYPTION KEY

FIG. 9